Appl. No. 09/896,197   Page 2 of 9
Amendment and/or Response
Reply to Office action of 5 April 2005

Amendments to the Claims:

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Cancelled).

2. (Currently amended) A method ~~as claimed in claim 1~~ for cryptographically converting an input data block into an output data block; the method including:

selecting a select permutation from a predetermined set of at least two permutations, and

performing a non-linear substitution operation on the input data block based on the select permutation,

wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set.

3. (Currently amended) A method as claimed in claim ~~1~~ 2, wherein

the data block consists of n data bits and

each permutation of the set of permutations is a set of 2^n elements, where each non-trivial differential characteristic of each permutation in this set has a probability that is less than or equal to a maximum probability;

the set of permutations being formed by permutations which have been selected such that for each non-trivial differential characteristic having the maximum probability in any of the permutations, this differential characteristic has a lower probability in at least one of the other permutations of the set.

4. (Original) A method as claimed in claim 3, wherein the differential characteristic has a probability equal to zero in at least one of the permutations.

Appl. No. 09/896,197
Amendment and/or Response
Reply to Office action of 5 April 2005

Page 3 of 9

5. (Previously presented) A method as claimed in claim 4, wherein $n = 4$, and the maximum probability equals ¼.

6. (Currently amended) A method as claimed in claim ~~1~~ 2, wherein

the data block consists of n data bits and

each permutation of the set of permutations is a set of 2^n elements, where each non-trivial linear characteristic of each permutation in this set has a probability of at least a minimum probability and at most a maximum probability,

the set of permutations being formed by permutations which have been selected such that for each non-trivial linear characteristic with probability that equals the minimum or maximum probability in any of the permutations, this linear characteristic has a probability closer to ½ in at least one of the other permutations of the set.

7. (Previously presented) A method as claimed in claim 6, wherein the linear characteristic has a probability equal to ½ in at least one of the permutations.

8. (Previously presented) A method as claimed in claim 6, wherein $n = 4$, the minimum probability is ¼, and the maximum probability is ¾.

9. (Currently amended) A method as claimed in claim ~~1~~ 2, wherein the set of permutations consists of two permutations.

10. (Currently amended) A method as claimed in claim ~~1~~ 2, wherein

selecting the select permutation is based on an encryption key.

11. (Previously presented) A method as claimed in claim 9, wherein

selecting the permutation is performed under control of a bit of an encryption key.

12. (Currently amended) A computer program product where the program product is operative to cause a processor to perform the method of claim ~~1~~ 2.

Appl. No. 09/896,197   Page 4 of 9
Amendment and/or Response
Reply to Office action of 5 April 2005

13. (Previously presented) A system for cryptographically converting an input data block
into an output data block; the system including:

    - an input for receiving the input data block;

    - a storage for storing a predetermined set of at least two permutations associated
with an S-box;

    - a cryptographic processor for performing a non-linear operation on the input
data block using an S-box based on a permutation; the processor being operative to, each
time before using the S-box, (pseudo-)randomly selecting the permutation from the stored
set of permutations associated with the S-box; and

    - an output for outputting the processed input data block.

14. (Previously presented) A cryptographic encoder comprising:

    one or more encryption stages,

    each stage of the one or more encryption stages including

        a non-linear substitution module that is configured to receive a control
signal and a set of data bits,

    wherein

    the non-linear substitution module includes a plurality of substitution boxes; and

    each of the substitution boxes is configured to receive at least a subset of the
control signal and a subset of the set of data bits, and:

        substitutes a first output value for the subset of the set of data bits if the
subset of the control signal is a first value, and

        substitutes a second output value for the subset of the set of data bits if the
subset of the control signal is a second value.

15. (Previously presented) The cryptographic encoder of claim 14, wherein

    each stage of the one or more encryption stages further includes

        an addition module that is configured to combine at least a subset of a key
with a data input to provide the set of data bits to the non-linear substitution module.

NL-000365 Final 5.405   Atty. Docket No. NL-000365

Appl. No. 09/896,197　　　　　　　　　　　　　　　　　　　　　　Page 5 of 9
Amendment and/or Response
Reply to Office action of 5 April 2005

16. (Previously presented) The cryptographic encoder of claim 15, wherein

the control signal includes another subset of the key.

17. (Previously presented) The cryptographic encoder of claim 15, wherein

each stage of the one or more encryption stages further includes

a transformation module that is configured to transform the output values

from the substitution boxes to provide therefrom an encrypted data output.

18. (Previously presented) The cryptographic encoder of claim 14, wherein

the second output value is formed such that a cryptographic weakness in the first

value is at least partially compensated by a corresponding cryptographic strength in the

second output value.

19. (Previously presented) The cryptographic encoder of claim 14, wherein

the subset of the set of data bits consists of n data bits and

each of the first and second data output values is a mapping of the subset of the

set of data bits to an element of a set of 2^n elements, where each non-trivial differential

characteristic of each of the set of 2^n elements of the first and second output values has a

probability that is less than or equal to a maximum probability;

the set of 2^n elements that provide second data output value being selected such

that for each non-trivial differential characteristic having the maximum probability in the

set of 2^n elements that provide the first output value, this differential characteristic has a

lower probability in the set of 2^n elements that provide second data output value.

Appl. No. 09/896,197   **Page 6 of 9**
Amendment and/or Response
Reply to Office action of 5 April 2005

20. (Previously presented) The cryptographic encoder of claim 14, wherein

the subset of the set of data bits consists of n data bits and

each of the first and second data output values is a mapping of the subset of the set of data bits to an element of a set of 2^n elements, where each non-trivial differential characteristic of each of the set of 2^n elements of the first and second output values has a probability that is at least a minimum probability and at most a maximum probability;

the set of 2^n elements that provide second data output value being selected such that for each non-trivial linear characteristic that equals the minimum or maximum probability in the set of 2^n elements that provide the first output value, this linear characteristic has a probability closer to $\frac{1}{2}$ in the set of 2^n elements that provide second data output value.